ON ALGEBRAIC GALOIS EXTENSIONS OF SIMPLE RINGS

TAKASI NAGAHARA*

Throughout the present paper, R will be a simple ring, S a simple subring of R (with common 1). And V, C, and Z represent $V_R(S)$, $V_R(R)$ and $V_S(S)$ respectively. If M is a unitary R-left (right) module, $[M|R]_l$ ($[M|R]_r$) will denote the uniquely determined number (finite or infinite) of irreducible direct summands of M. When R is Galois over S, we denote by $\mathfrak{G}$ the Galois group of R/S. And, as to notations and terminolgies used in this paper, we follow the previous one [4]. The writer is grateful to Dr. H. Tominaga for his kind advices.

In case R is a division ring, we proved that if R is Galois, left algebraic and of bounded degree over a division subring S then R is finite over S [3, Theorem 4]. Afterwards, in case S is a central simple algebra of finite rank, this result has been extended to simple rings [4, Theorem 5.2]. One of the purposes of this paper is to present the complete extension of [3, Theorem 4] to simple rings:

Theorem 1. *If R is Galois, left algebraic and of bounded degree over S then R is finite over S.*

Next, we shall prove a theorem which is a partial extension of [3, Theorem 3] and [4, Theorem 5.1]:

Theorem 2. *If R is Galois and left algebraic over S then R is locally finite over S, provided the Galois group $\mathfrak{G}$ of R/S is almost outer (, whence $\mathfrak{G}$ is locally finite).*

For the proofs of our principal theorems, several lemmas will be needed. At first we shall prove the following:

Lemma 1. *Let S be a division subring of R. N a Z-right submodule of R with $[N:Z]_r<\infty$. If $[S:Z]=\infty$ then for each positive integer q there exist q non-zero elements $s_1, \cdots, s_q \in S$ such that $\sum_{i=1}^q Ns_i=\sum_{i=1}^q \oplus Ns_i$.*

Proof. Patterning after the latter half of the proof of [4, Lemma 6.6] or the proof of [2, Lemma 3] according as S is algebraic or transcendental over Z (V should be replaced by Z), one will easily obtain our lemma. And so, the details may be left to readers.

Lemma 2. *Let R/S be Galois, S' an intermediate ring of R/S such*

---
* Yukawa Fellow of Osaka University in 1961.

that R is S'-R-irreducible, and let $M\neq 0$ be an S-S'-submodule of R.

(i) *$(\sigma|M)R_r$ is S'_r-R_r-irreducible and R_r-isomorphic to R_r for each $\sigma\in\mathfrak{G}$.*

(ii) *For any subset $\mathfrak{B}$ of $\mathfrak{G}|M$, $\mathfrak{B}$ is linearly independent over R_r if and only if so it is over V_r.*

(iii) *$(\mathfrak{G}|M)R_r$ possesses a subset of $\mathfrak{G}|M$ as a linearly independent R_r-basis, and $\mathfrak{B}\subseteq\mathfrak{G}|M$ is a linearly independent R_r-basis of $(\mathfrak{G}|M)R_r$ if and only if it is a linearly independent V_r-basis of $(\mathfrak{G}|M)V_r$.*

Proof. (i) Let x be an arbitrary non-zero element of R. Then, by our assumption, there holds $S'_r(\sigma|M)x_rR_r=(\sigma|M)(S'\sigma xR)_r=(\sigma|M)\{(S'x\sigma^{-1}R)\sigma\}_r=(\sigma|M)R_r$, whence our assertion is clear.

(ii) Let a subset $\mathfrak{B}$ of $\mathfrak{G}|M$ be linearly dependent over R_r, and let $\sum_{i=1}^t(\sigma_i|M)x_{ir}=0$ ($x_i\in R$) be a non-trivial relation of the shortest length. Then, by (i), we obtain $\sigma_1|M=\sum_{i=2}^t(\sigma_i|M)y_{ir}$ for some $y_i\in R$. Here, by making use of the standard argument, one can easily see that each y_i is contained in V. Hence, we have proved that $\mathfrak{B}$ is linearly dependent over V_r. And the converse is trivial.

(iii) This is an easy consequence of (i) and (ii).

By the validity of Lemma 2, we can prove the following useful inequalities.

Lemma 3. *Let R/S be Galois, and S' an intermediate ring of R/S such that R is S'-R-irreducible. If M is an S-S'-submodule of R with $[M|S]_l<\infty$ then for each $a\in M$ there holds*

$$m\cdot[a\mathfrak{G}V_r|V]_r<mm'+m'\cdot[M|S]_l,$$

where $m=[S|S]$ and $m'=[V|V]$ are the capacities of S and V respectively. In particular, if S is a division ring, we have

$$\frac{1}{m'}[a\mathfrak{G}V_r|V]_r<1+[M:S]_l$$

Proof. By Lemma 2 (i) and (ii), there holds $m\cdot[a\mathfrak{G}V_r|V]_r\leqq m\cdot[(\mathfrak{G}|M)V_r|V_r]_r=mm'\cdot[(\mathfrak{G}|M)V_r:V_r]_r=mm'\cdot[(\mathfrak{G}|M)R_r:R_r]_r$. Thus, to complete our proof, it suffices to prove the nxet:

$$m\cdot[(\mathfrak{G}|M)R_r:R_r]_r<m+[M|S]_l.$$

Now, we can find a S-left submodule M' of R such that $[M'|S]_l<m$, $M^*=M+M'=M\oplus M'$, and that M^* possesses a linearly independent S-left basis. Then, by Lemma 2 (i), we obtain

$$[M^*:S]_l=[\mathrm{Hom}_{S_l}(M^*,R):R_r]_r\geqq[(\mathfrak{G}|M)R_r:R_r]_r.$$

Consequently, there holds $[M|S]_l+m>[M|S]_l+[M'|S]_l\geqq$

$m \cdot [(\mathfrak{G} | M)R_r : R_r]_r$.

Now, we shall prove the following lemma which will play an essential role in our present study.

Lemma 4. *If R/S is Galois, left algebraic and of bounded degree then $[R:S]<\infty$, provided there exists an intermdiate ring S' of R/S with $[S':S]_l<\infty$ such that R is S'-R-irreducible.*

Proof. At first, we shall remark that V is finite over Z. For, noting that $S[V]=S\times_Z V$, we readily see that V is an algebraic algebra over Z and of bounded degree, and so $[V:V_V(V)]<\infty$ by [1, Theorem 7·11·1]. Moreover, V/Z being Galois, it will be easy to see that $V_V(V)$ is finite over Z. Hence, it follows $[V:Z]<\infty$.

Let $S=\sum_{i,j=1}^{m} S_0 f_{ij}$, where f_{ij}'s are matrix units and $S_0=V_S(\{f_{ij}\text{'s}\})$ is a division ring. Then, as is well-known, $S'=\sum_{i,j=1}^{m} S_0' f_{ij}$ and $R=\sum_{i,j=1}^{m} R_0 f_{ij}$ for $S_0'=V_{S'}(\{f_{ij}\text{'s}\})$ and the simple ring $R_0=V_R(\{f_{ij}\text{'s}\})$. Here, one will easily see that R_0/S_0 is Galois, left algebraic and of bounded degree, and that R_0 is S_0'-R_0-irreducible. Further, our assertion for the case $[S:Z]<\infty$ has been proved in [4, Theorem 5·2]. Thus, in what follows, we may, and shall, restrict our proof to the case where S *is a division ring and* $[S:Z]=\infty$.

Let $S'=Su_1+\cdots+Su_p$, and $s=\mathrm{Max}_{x\in R}\{[S[x]:S]_l\}$. And let t be an integer such that $t\geqq 1+ps$. Now, we suppose that $[R:S]_l=\infty$. As, to be easily verified, $\mathfrak{G}R_r$ is two-sided simple, if $[\mathfrak{G}R_r:R_r]_r<\infty$ then one can easily see that $[R:S]<\infty$. This contradiction shows that $[\mathfrak{G}R_r:R_r]_r=\infty$. And so, there exist some $\sigma_1,\cdots,\sigma_t\in\mathfrak{G}$ such that $\{\sigma_1,\cdots,\sigma_t\}$ is linearly independent over R_r. If x is an element of R, $SxS'=Sx(Su_1+\cdots+Su_p)\subseteq S[x]u_1+\cdots+S[x]u_p$ yields

$$(1)\qquad [SxS':S]_l\leqq sp.$$

Here, choose an arbitrary S-S'-submodule M_0 of R with $[M_0:S]_l<\infty$. If $[\sum_{i=1}^{t}(\sigma_i|M_0)R_r:R_r]_r<t$ (cf. Lemma 2 (i)), then there holds a non-trivial relation: $\sum_{i=1}^{t}(\sigma_i|M_0)a_{ir}=0$ $(a_i\in R)$. Since $\alpha=\sum_{i=1}^{t}\sigma_i a_{ir}\neq 0$, there exists some $b_1\in R$ such that $b_1\alpha\neq 0$. We set here $M_1=M_0+Sb_1S'$. Then, by (1) we have $[M_1:S]_l<\infty$. And $M_1\alpha\neq 0$ implies $[\sum_{i=1}^{t}(\sigma_i|M_0)R_r:R_r]_r<[\sum_{i=1}^{t}(\sigma_i|M_1)R_r:R_r]_r$. Thus, repeating the same procedures, we can find eventually an S-S'-submodule $M=Sd_1+\cdots+Sd_q$ of R such that $t=[\sum_{i=1}^{t}(\sigma_i|M)R_r:R_r]_r$. Recalling the fact $[V:Z]<\infty$ remarked at the opening, we see that $N=\sum_{i,j}(d_j\sigma_i)V$ is right-finite over Z. And so, by Lemma 1, there exist some non-zero $s_1,\cdots,s_q\in S$ such that

$$(2)\qquad \sum_{j=1}^{q} Ns_j=\sum_{j=1}^{q}\oplus Ns_j.$$

We set here $a=\sum_{j=1}^{q} d_j s_j$ ($\in M$). If $\sum_{i=1}^{t}(a\sigma_i)v_i=0$ ($v_i\in V$), then $\sum_{j=1}^{q}(d_j\alpha')s_j=a\alpha'=\sum_{i=1}^{t}(a\sigma_i)v_i=0$, where $\alpha'=\sum_{i=1}^{t}(\sigma_i|M)v_{i_r}$. Noting that $d_j\alpha'\in N$, there holds $d_j\alpha'=0$ ($j=1,\cdots,q$) by (2). And this implies $M\alpha'=\sum_{j=1}^{q}S(d_j\alpha')=0$, that is, $0=\alpha'=\sum_{i=1}^{t}(\sigma_i|M)v_{i_r}$. Since $\{\sigma_1|M,\cdots,\sigma_t|M\}$ is linearly independent over V_r, we have $v_i=0$ ($i=1,\cdots,t$). We have proved therefore that $a\sigma_1,\cdots,a\sigma_t$ is linearly independent over V. Accordingly, by (1) and Lemma 3 we obtain

$$1+ps\geqq 1+[SaS':S]_l>\frac{1}{m'}[a\mathfrak{G}V_r|V]_r\geqq[\textstyle\sum_{i=1}^{t}(a\sigma_i)V:V]_r=t,$$

where m' is the capacity of V. But this contradicts $t\geqq 1+ps$, and our proof is complete.

Lemma 5: *Let R/S be Galois and left algebraic. If $\mathfrak{G}$ is almost outer and S' is an intermediate ring of R/S with $[S':S]_l<\infty$ such that R is S'-R-irreducible then for each $x\in S'$ we have $\#\{x\mathfrak{G}\}<\infty$*[1].

Proof. Since $\mathfrak{G}$ is almost outer, i. e. $(V^*:C^*)$ (the group index of the multiplicative group C^* of non-zero elements of C in the multiplicative group V^* of regular elements of V)$<\infty$, V is finite or $V=C$ by [6, Lemma 1]. In virtue of Lemma 2 (i), we have

$$\infty>[S':S]_l=[\mathrm{Hom}_{S_l}(S'.R):R_r]_r\geqq[(\mathfrak{G}|S')R_r:R_r]_r.$$

And so, we can set $(\mathfrak{G}|S')R_r=\sum_{i=1}^{t}\oplus(\sigma_i|S')R_r$ with some $\sigma_i\in\mathfrak{G}$. Then, by Lemma 2 (iii), $\{\sigma_1|S',\cdots,\sigma_t|S'\}$ is a linearly independent V_r-basis of $(\mathfrak{G}|S')V_r$: $(\mathfrak{G}|S')V_r=\sum_{i=1}^{t}\oplus(\sigma_i|S')V_r$. If V is finite, our assertion is clear by the last representation. Thus, in what follows, we may, and shall restrict our proof to the case $V=C$. Now, let σ be an arbitrary element of $\mathfrak{G}$. Then $\sigma|S'=\sum_{i=1}^{t}(\sigma_i|S')v_{i_r}$ ($v_i\in V$). And so, for each $x\in S'$ we have

$$x_r(\sigma|S')=\begin{cases}(\sigma|S')(x\sigma)_r=\sum_{i=1}^{t}(\sigma_i|S')(v_i(x\sigma))_r=\sum_{i=1}^{t}(\sigma_i|S')((x\sigma)v_i)_r,\\ x_r\sum_{i=1}^{t}(\sigma_i|S')v_{i_r}=\sum_{i=1}^{t}(\sigma_i|S')((x\sigma_i)v_i)_r.\end{cases}$$

Hence, we obtain $\sum_{i=1}^{t}(\sigma_i|S')\{(x\sigma-x\sigma_i)v_i\}_r=0$, whence it follows $(x\sigma-x\sigma_i)v_i=0$ ($i=1,\cdots,t$). Noting that some of v_i's, say v_1, is non-zero, we see that $x\sigma=x\sigma_1$. We have proved therefore that $x\mathfrak{G}=\{x\sigma_1,\cdots,x\sigma_t\}$.

Now, let R be represented as $\sum_{i,j=1}^{n}De_{ij}$ with matrix units e_{ij}'s and a division ring $D=V_R(\{e_{ij}\text{'s}\})$. If $n>1$ and S contains an element $a=\sum_{i,j=1}^{n}c_{ij}e_{ij}$ with $c_{pq}\neq 0$ for some $p\neq q$ then, for an arbitrary permutation

$$\begin{pmatrix}1 & 2 & \cdots & n-1 & n\\ p_1 & p_2 & \cdots & p_{n-1} & p_n\end{pmatrix}$$

1) For any E, $\#(E)$ will signify the cardinal number of E.

such that $p_1=p$ and $p_n=q$, $e'_{ij}=e_{p_ip_j}$ can be adopted as new matrix units of R and $e'_{1n}=e_{pq}$. Accordingly, without loss of generality, we may assume that $c_{1n}\neq 0$. On the other hand, if $n>1$ and every element of S is diagonal, it is clear that all $e_{ii}\in V$. Hence, $V=\sum_{i=1}^{n}\oplus e_{ii}V$. If moreover V is a simple ring, the last fact means $[V|V]\geqq[R|R]$. Since $[V|V]\leqq[R|R]$ trivially, $[V|V]=[R|R]$. Accordingly, if $V=\sum_{i,j=1}^{n}E'e'_{ij}$ with matrix units e'_{ij}'s and a division ring $E'=V_V(\{e'_{ij}\text{'s}\})$, then $R=\sum_{i,j=1}^{n}D'e'_{ij}$ with the division ring $D'=V_R(\{e'_{ij}\text{'s}\})$. Thus, to prove our principal theorems, it will suffice to restrict our subsequent consideration to the following three cases:

Case I. $n=1$.
Case II. $n>1$ *and S contains an element* $a=\sum_{i,j=1}^{n}c_{ij}e_{ij}$ *with* $c_{1n}\neq 0$.
Case III. $n>1$ *and* $S\subseteq D$.

Lemma 6. *Let Case* II *happen.*

(i) *Let* $\begin{pmatrix}1 & 2 & \cdots & n-1 & n\\ p_1 & p_2 & & p_{n-1} & p_n\end{pmatrix}$ *be an arbitrary permutation snch that* $p_1=1$ *and* $p_n=n$, *and* $x_2,\cdots,x_n$ *arbitrary non-zero elements of D. If* $r=\sum_{i=2}^{n}x_ie_{p_ip_{i-1}}$ *then R is $S[r]$-R-irreducible.*

(ii) *If* $D\neq GF(2)$ *then* $R=S[F]$, *where F is the set of elements R such that R is $S[r]$-R-irreducible.*

Proof. (i) If we set $e'_{ij}=e_{p_ip_j}$ then $e'_{1n}=e_{1n}$ and $r=\sum_{i=2}^{n}x_ie'_{ii-1}$. And so, without loss of generality, we may assume that the permutation is identical. Let M be an arbitrary non-zero $S[r]$-R-submodule. Then, M contains an element $b=\sum_{i=p}^{n}d_ie_{in}$ with $d_p\neq 0$ for some p. Since $M\ni r^{n-p}b$ $=x_n\cdots x_{p+1}d_pe_{nn}$ (if $p=n$, $M\ni b=d_ne_{nn}$), e_{nn} is contained in M, whence it follows $M\ni ae_{nn}=\sum_{i=1}^{n}c_{in}e_{in}$. Hence, there holds $M\ni r^{n-k}\sum_{i=1}^{n}c_{in}e_{in}=$ $\sum_{i=2}^{k}x_{n-k+i}\cdots x_{i+1}c_{in}e_{n-k+i,n}+x_{n-k+1}\cdots x_2c_{1n}e_{n-k+1,n}$ $(k=1,\cdots,n)$. Recalling that $c_{1n}\neq 0$, one can see inductively that $e_{nn},e_{n-1n},\cdots,e_{1n}\in M$, whence eventually $e_{ij}\in M$. Now, it will be easy to see that $M=R$.

(ii) Let $\begin{pmatrix}1 & 2 & \cdots & n-1 & n\\ p_1 & p_2 & & p_{n-1} & p_n\end{pmatrix}$ be an arbitrary permutation such that $p_1=1$ and $p_n=$ n, and let x be an arbitrary non-zero element of D. Then, by (1) $F\ni r_{x,i}=e_{p_np_{n-1}}+\cdots+xe_{p_ip_{i-1}}+\cdots+e_{p_2p_1}$ $(2\leqq i\leqq n)$. Since there exists an element $z\in D$ different from 1 and 0, $S[F]\ni r_{z,i}-r_{z-1,i}=e_{p_ip_{i-1}}$ $(2\leqq i\leqq n)$. Further for arbitrary $y\in D$ different from 1 and 0 we obtain $S[F]\ni$ $r_{1,i}-r_{1-y,i}=ye_{p_ip_{i-1}}(2\leqq i\leqq n)$. Hence, noting that $xe_{n1}=xe_{nn-1}e_{n-1n-2}\cdots e_{21}$, we see that $S[F]\supset De_{nj}$ $(1\leqq j<n)$, $De_{ij}(1<i\neq j<n)$ and De_{i1} $(1<i\leqq n)$. Consequently,

$$(3)\quad S[F]\ni(\sum_{i,j=1}^{n}c_{ij}e_{ij})c_{1n}^{-1}xe_{nk} = c_{nn}c_{1n}^{-1}xe_{nk}+\sum_{i=2}^{n-1}c_{in}c_{1n}^{-1}xe_{ik}+xe_{1k}\ (1\leqq k<n).$$

Since for $n>k>1$ $S[F]$ contains $e_{k1}(\sum_{i,j=1}^{n}c_{ij}e_{ij})c_{1n}^{-1}de_{nk}=de_{kk}(d\in D)$, it will be easily seen that $S[F]\ni\sum_{i=2}^{n-1}c_{in}c_{1n}^{-1}xe_{ik}$. Hence, from (3), we obtain $xe_{1k}\in S[F]$ $(1\leqq k<n)$, in particular, $e_{11}\in S[F]$. And so, $S[F]$ contains $e_{nn}=1-\sum_{i=1}^{n-1}e_{i1}e_{1i}$ too, whence it follows $e_{1n}=c_{1n}^{-1}e_{11}(\sum_{i,j=1}^{n}c_{ij}e_{ij})e_{nn}\in S[F]$. Thus, we have proved that $e_{1j}\in S[F]$ $(1\leqq j\leqq n)$. Since $e_{i1}\in S[F]$ $(1\leqq i\leqq n)$, $e_{ij}\in S[F]$ and $D\subseteq S[F]$.

Lemma 7. *Let Case* III *happen, R/S be left algebraic and $S\not\subseteq C$ (whence $D\not\subseteq V$ by $D\supseteq S$).*

(i) *For an arbitrary $x\in D\backslash V$, if $r=\sum_{i=2}^{n}e_{i-1i}+xe_{n1}$ then R is $S[r]$-R-irreducible.*

(ii) $R=S[F]$, *where F is the set mentioned in Lemma* 6 (ii).

Proof. (i) Thers exists an element $y\in S$ wihth $xy\neq yx$. Since $r^{-1}=\sum_{i=2}^{n}e_{ii-1}+x^{-1}e_{1n}\in S[r]$, $S[r]$ contains $r^{n-i}(r-yry^{-1})(r^{-1}-yr^{-1}y^{-1})r^{-(n-j)}=(x-yxy^{-1})(x^{-1}-yx^{-1}y^{-1})e_{ij}$. Noting that $(x-yxy^{-1})(x^{-1}-yx^{-1}y^{-1})$ is a non-zero element of $S[r]\cap D$, it follows that $e_{ij}\in S[r]$ $(i,j=1,\cdots,n)$. Now the $S[r]$-R-irrducibility of R will be easy.

(ii) By (i), it is clear that e_{ij} $(i,j=1,\cdots,n)$ and arbitrary $x\in D\backslash V$ are contained in $S[F]$ (and so $x^{-1}\in S[F]$ as well). On the other hand, if c is a non-zero element of $D\cap V$ then $xc\in S[F]$ for arbitrary $x\in D\backslash V$, whence it follows $c\in S[F]$. Consequently, we obtain $R=\sum_{i,j=1}^{n}De_{ij}=S[F]$.

Now we can prove our principal theorems.

Proof of Theorem 1. For Case I, R being S-R-irreducible, our assertion is a direct consequence of Lemma 4. Next, for Case II it is easy by Lemma 6 (i) and Lemma 4. And finally, our asserion for Case III is contained in [4, Theorem 5.2] provided $S\subseteq C$, and for the case remained it is clear by Lmma 7 (i) and Lemma 4.

Proof of Theorem 2. If $D=GF(2)$, our assertion is trivial. For case 1, noting that R is always $S[r]$-R-irreducible for $r\in R$, $\mathfrak{G}$ is locally finite by Lemma 5. Similaily, for Case II and Case III, by making respective use of Lemma 6 and Lemma 7 together with Lemma 5 we see that $\mathfrak{G}$ is locally finite provided $D\neq GF(2)$ and $S\not\subseteq C$ respectively. Finally, if $n>1$ and $S\subseteq C$ then $V=R$ is finite by [6, Lemma 1] (for, $\mathfrak{G}$ is almost outer).

From Lemma 5, Theorem 2 and [5, Theorem 1.1 and Theorem 3.1] we obtain the following:

Corollary 1. *If R/S is left algebraic and outer Galois then, for any finite subset E of R,*

(i) $\#\{E\mathfrak{G}\}$ is finite,

(ii) *the ring* $S[E]$ *generated by* E *over* S *is a simple ring which is finite over* S,

(iii) $S[E]=S[a]$ *for some* $a\in S[E]$.

By Corollary 1, it will be easy to see that the infinite Galois theory of division rings [1, VII, § 6] of N. Jacobson can be extended to simple rings under the same assumptions such that R/S is left algebraic and outer Galois as in [1, VII, §6]. The following corollary[2)] is one of those extensions.

Corollary 2. *If* R/S *is left algebraic and outer Galois then there exists a* $1-1$ *dual correspondence between closed subgroups of* $\mathfrak{G}$ *and intermediate rings of* R/S, *in the usual sense of Galois theory.*

REFERENCES

[1] N. JACOBSON, Structure of rings, Providence (1956).

[2] T. NAGAHARA. On generating elements of Galois extensions of division rings IV, Math. J. Okayama Univ., 8 (1958), 181-188.

[3] T. NAGAHARA, On generating elements of Galois extensions of division rings V, Math. J. Okayama Univ., 10 (1960), 11—17.

[4] T. NAGAHARA and H. TOMINAGA, On Galois and locally Galois extensions of simple rings, Math. J. Okayama Univ., 10 (1961), 143—166.

[5] H. TOMINAGA, Galois theory of simple rings II, Math. J. Okayama Univ. 6 (1957), 153—170.

[6] H. TOMINAGA, A note on conjugates II, Math. J. Okayama Univ., 9 (1959), 1—3.

DEPARTMENT OF MATHEMATICS,

OKAYAMA UNIVERSITY.

(*Received January 24, 1962*)

2) This is a restatent of the latter part of [4, Corollary 1,4].